

Testing network segmentation

The idea is to test if users from a Guest-network can reach another, more sensitive network.

It might be that the networks are separated by a firewall.

Tests

- Test reach to machine using icmp

```
sudo hping3 -1 10.10.10.10
# with traceroute
sudo hping3 --traceroute -V -1 10.10.10.10
```

- Test reach machine using SYN packet

You need to test against a machine and port that will respond to a syn packet

```
-S is for SYN packet
-p is for destination port
-s is for source port
sudo hping3 -V -S -p 80 -s 5050 10.10.10.10
sudo hping3 -V -S -p 80 -s 53 10.10.10.10
sudo hping3 --traceroute -V -S -p 80 -s 53 10.10.10.10
```

- Test reach machine over icmp with ipv6

```
sudo ping6 fe80::7041:bba0:593f:c6a5%11
```